



**NASA Code Q  
Risk Management Colloquium  
25 - 26 October 2004**

**Risk Management for the  
Cassini/Huygens Mission to Saturn  
and Titan**

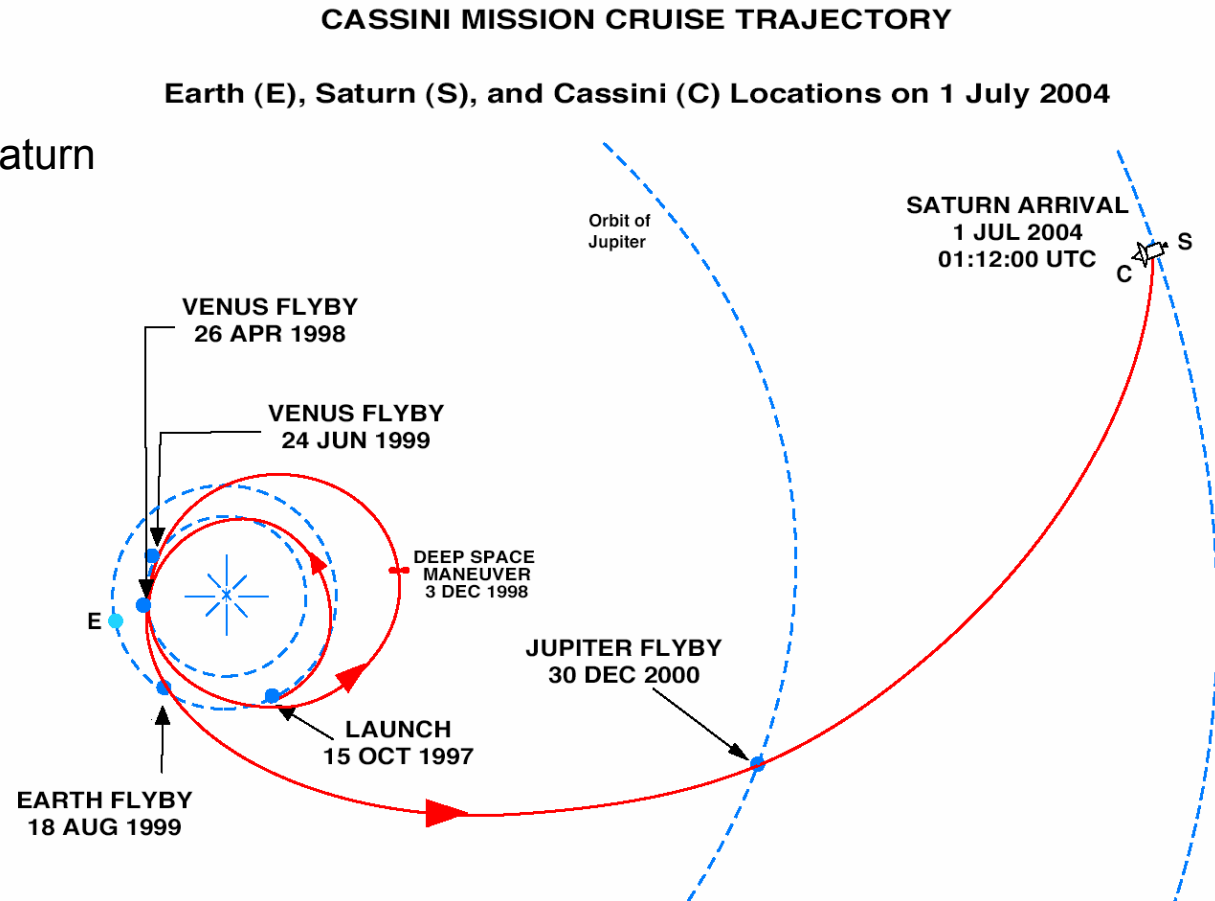
**Mona M. Witkowski  
Robert T. Mitchell  
25 October 2004**

# Earth to Saturn

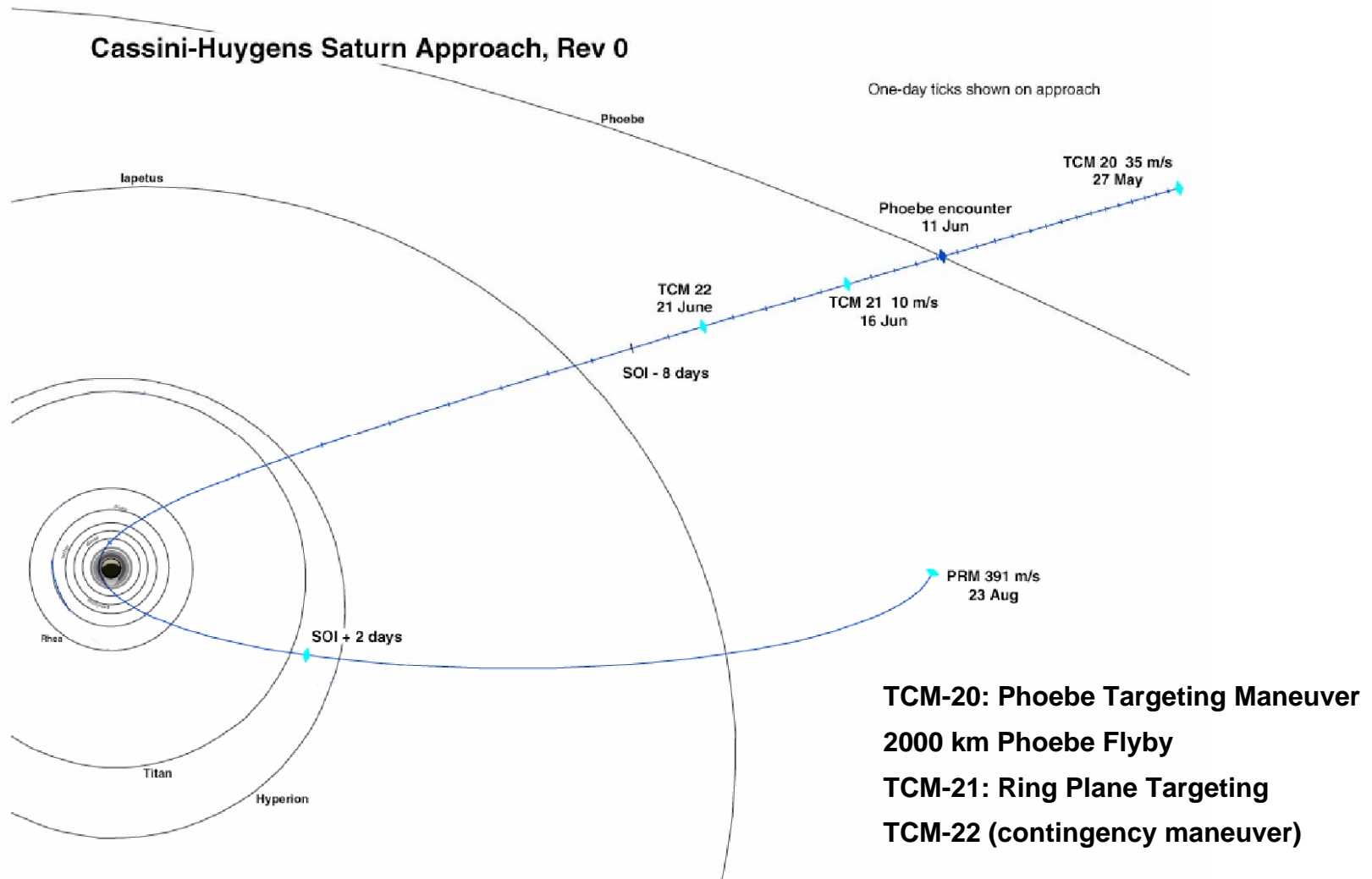
- Cassini/Huygens is a joint NASA/ESA/ASI mission to Saturn
- Launched October 15, 1997



- Saturn Orbit Insertion (SOI)
  - July 1, 2004 01:12 UTC
- Probe Release 12/24/04
  - Probe Relay 1/14/05



# Near Saturn

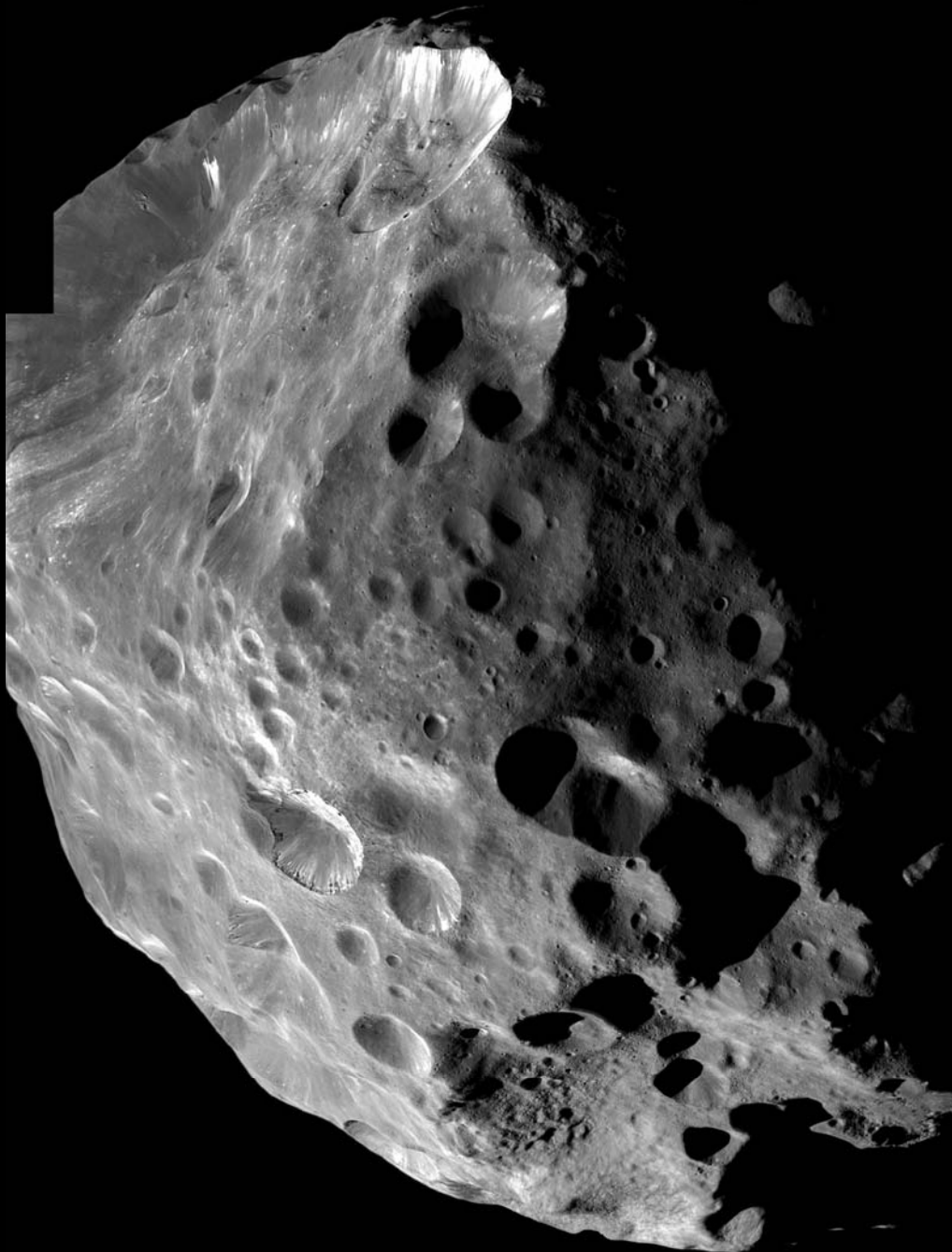


# Phoebe as seen by Voyager



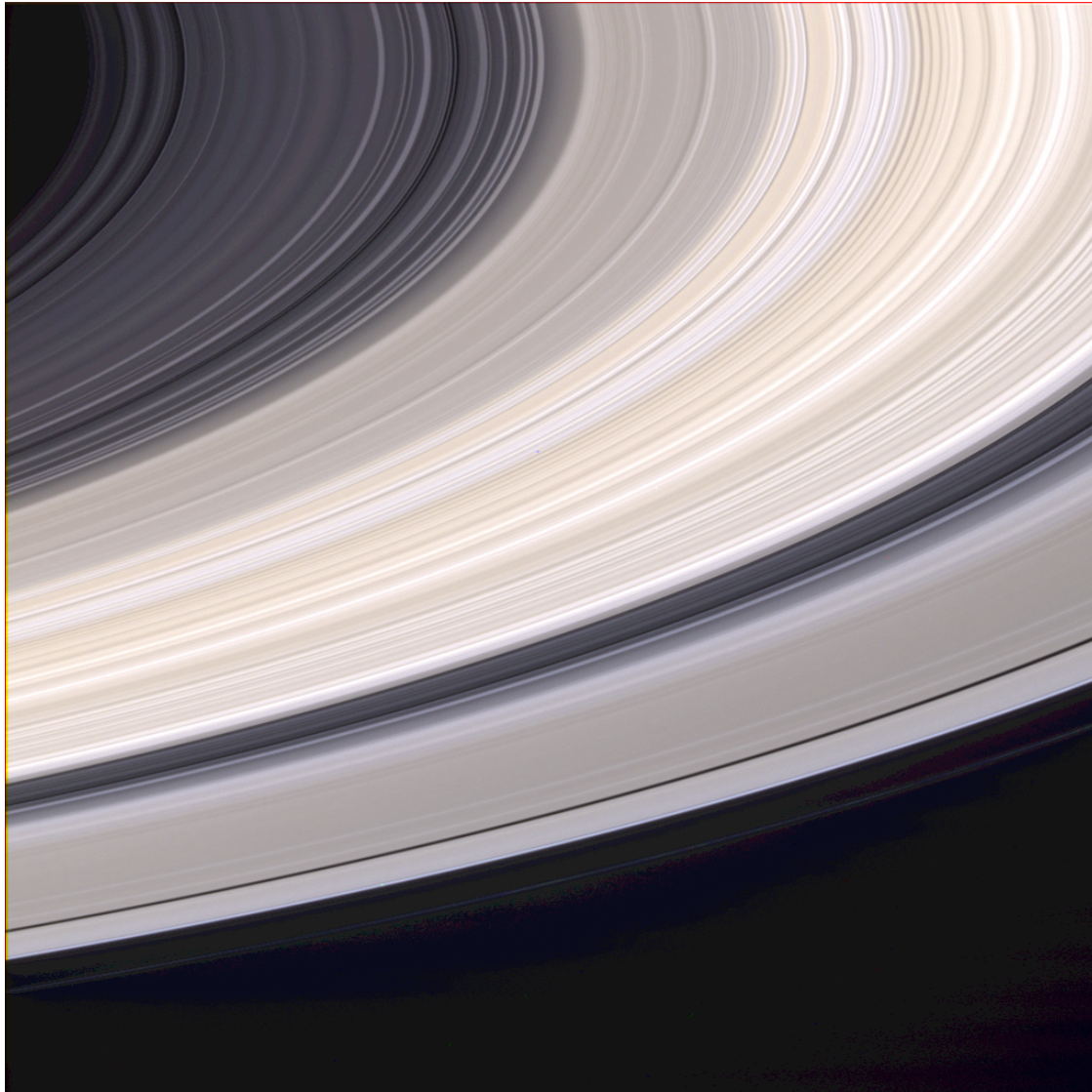


The Face of  
Phoebe



Phoebe High-  
Resolution Mosaic

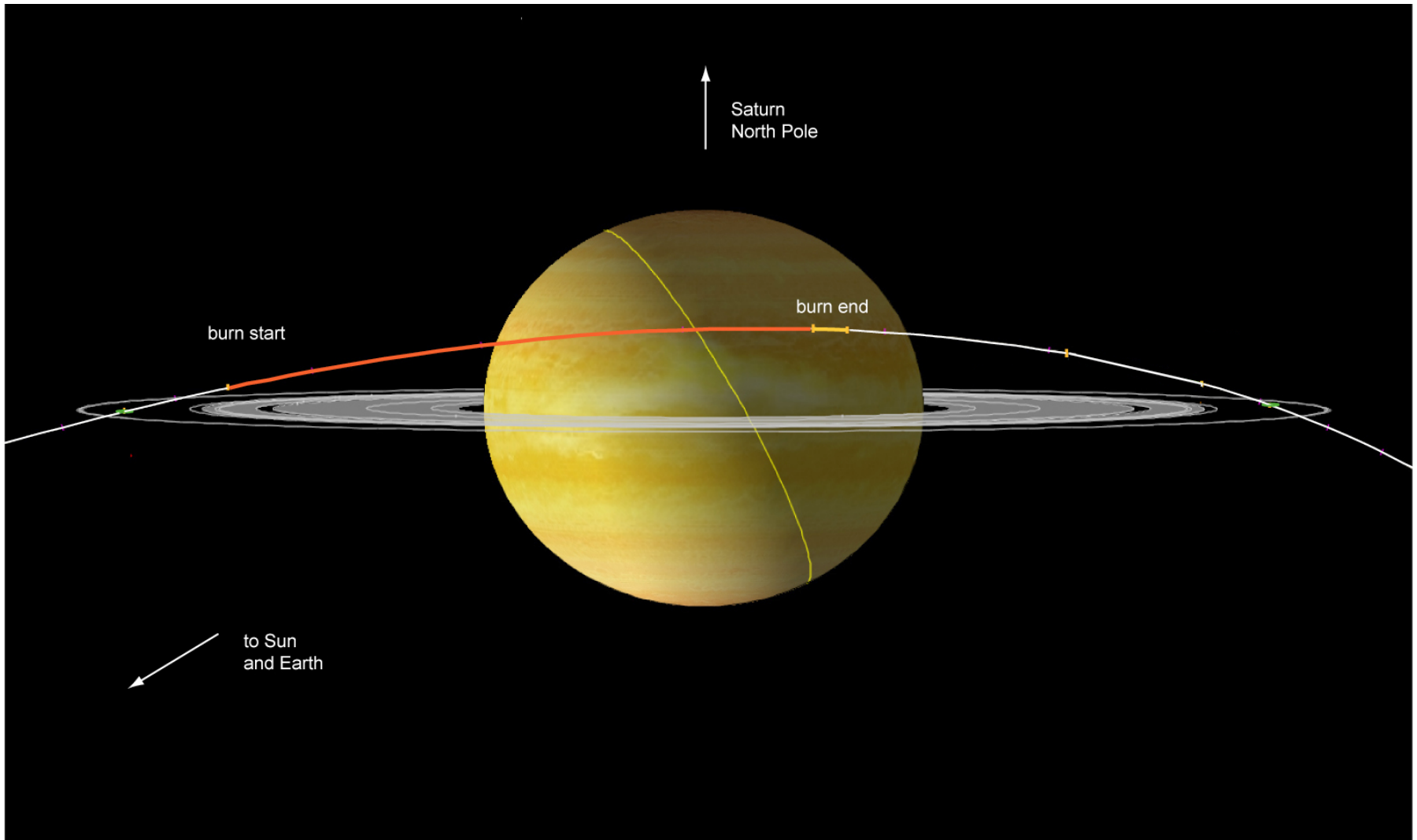
# The View on Approach to SOI



October 25, 2004

R. T. Mitchell

# SOI Geometry

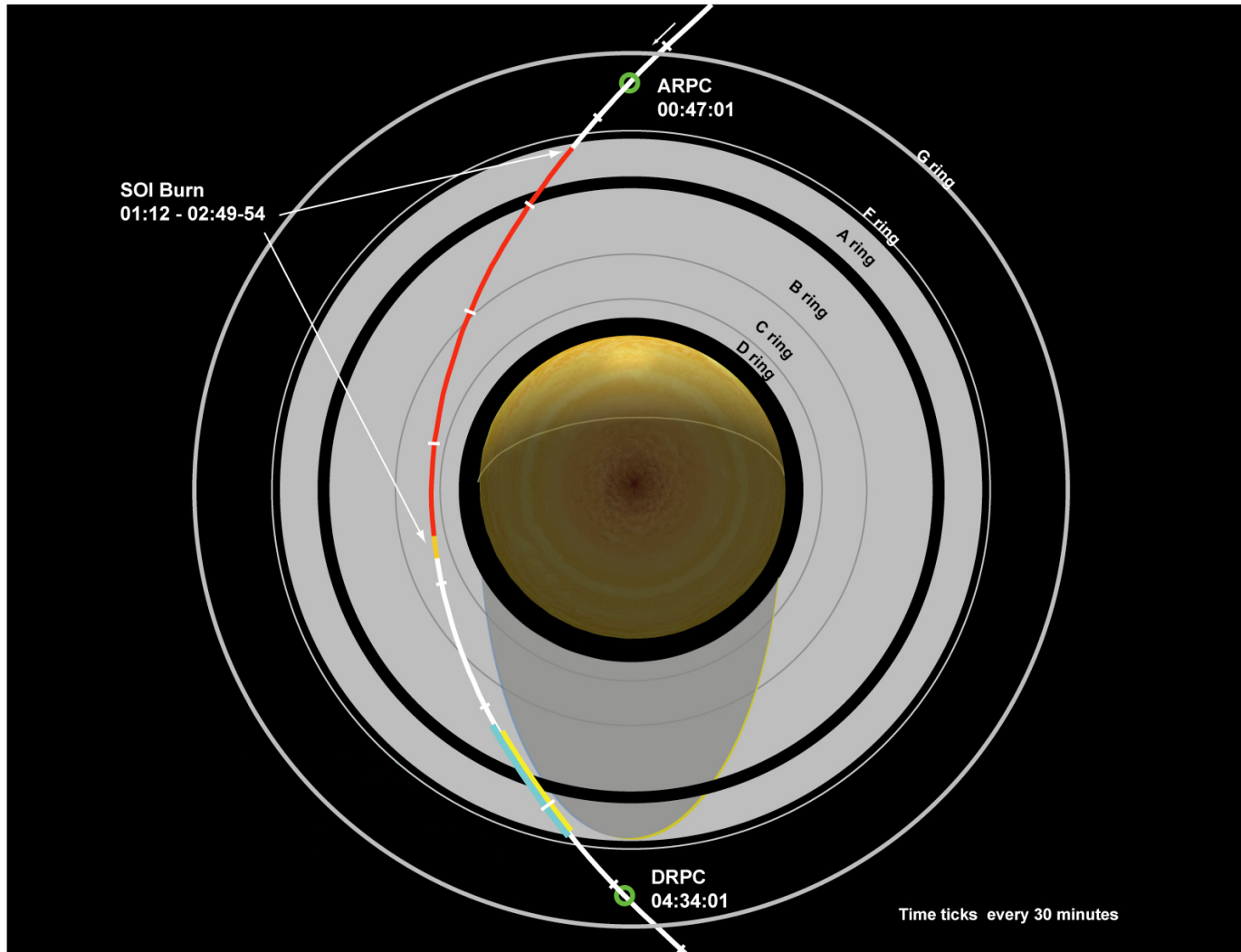


October 25, 2004

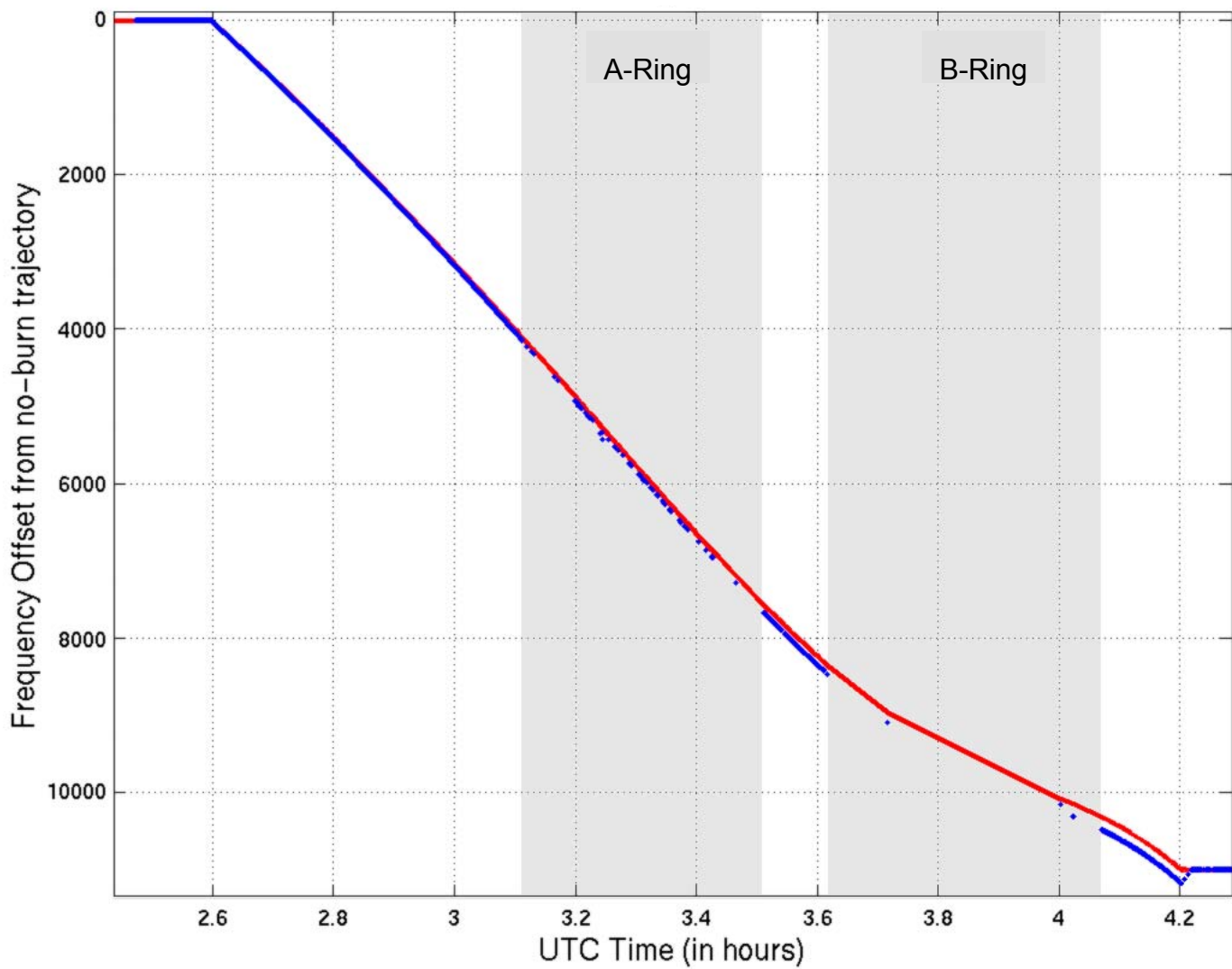
R. T. Mitchell

# SOI Geometry

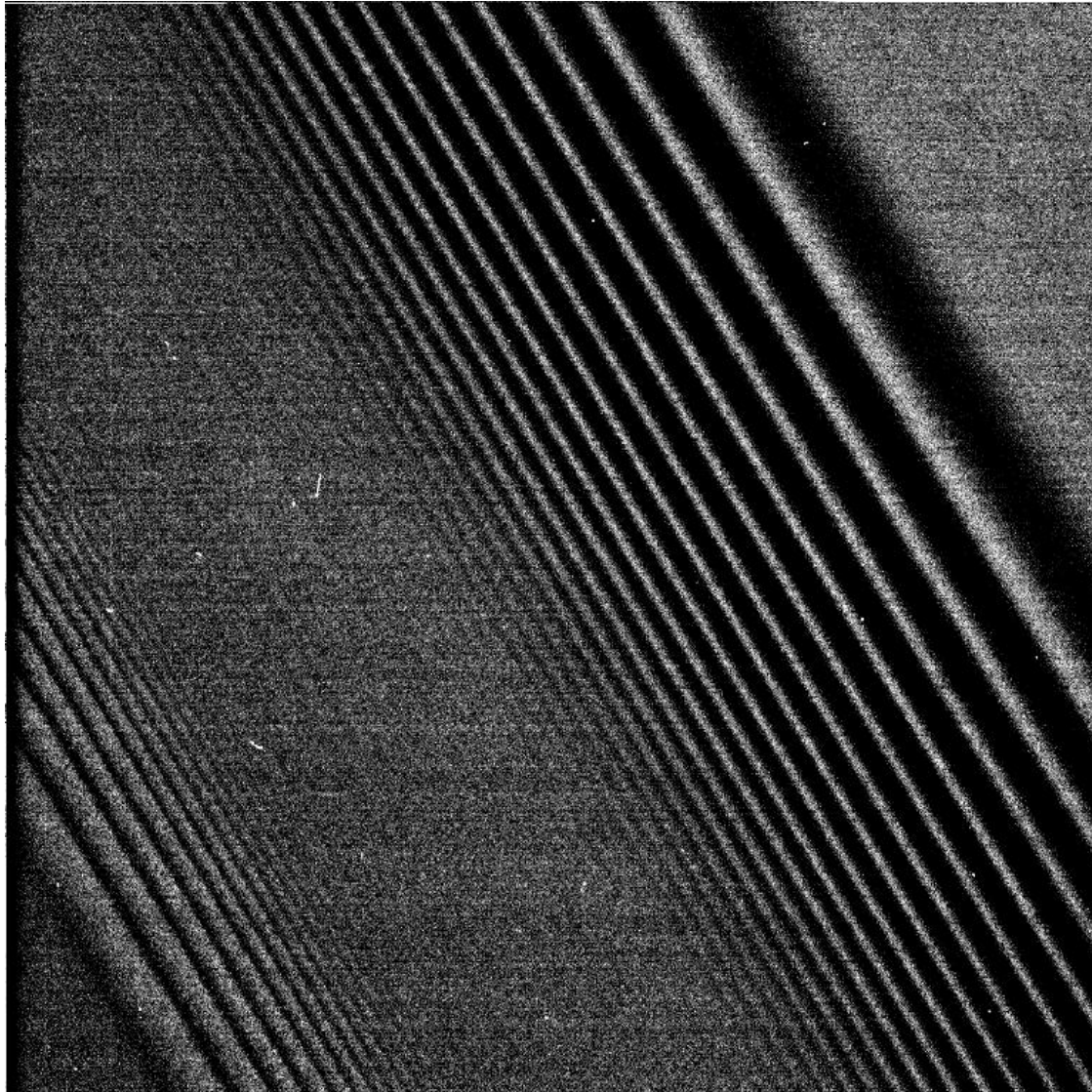
(Continued)



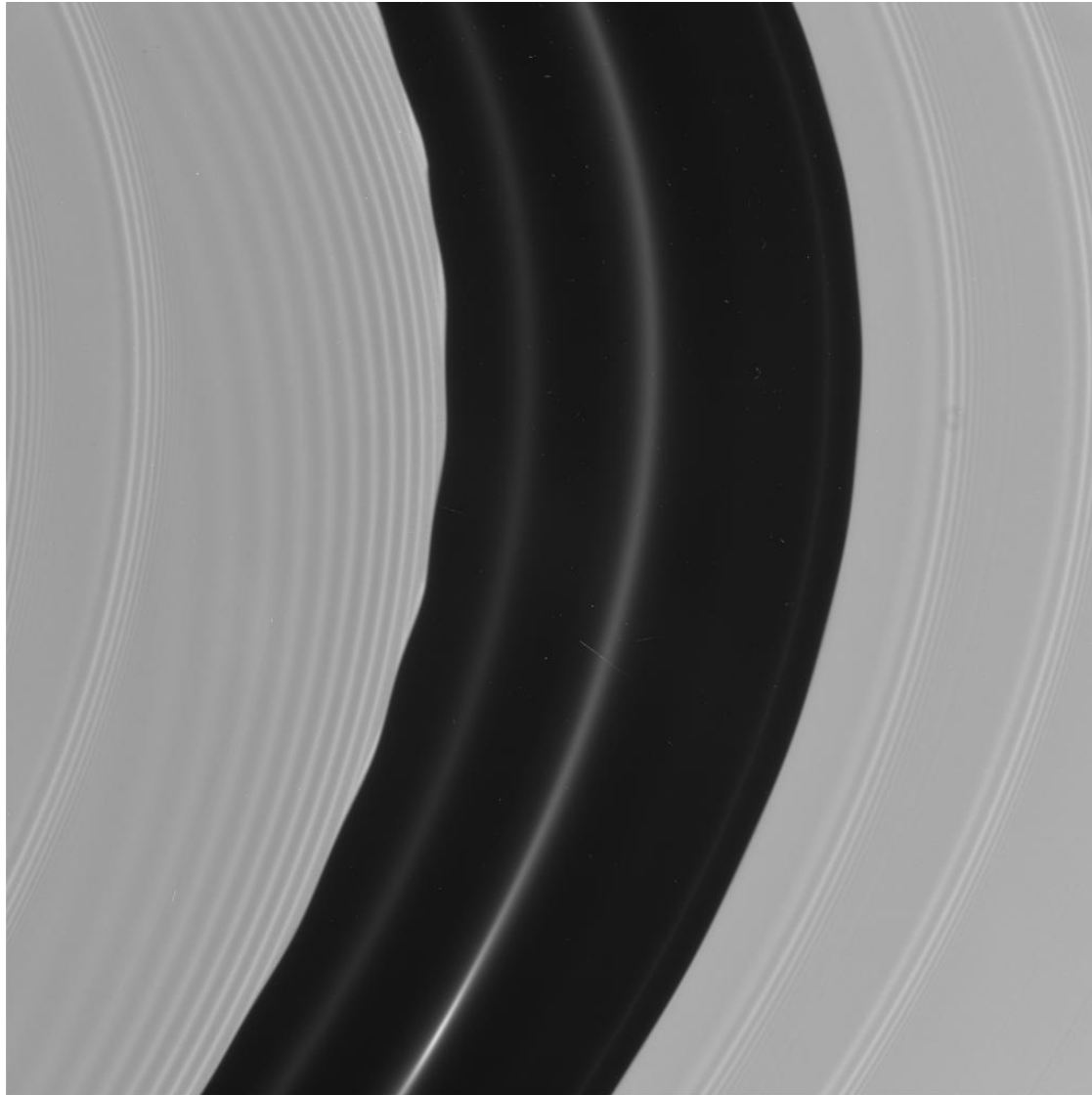
# SOI Doppler Shift



# Two Waves in one Ring Image



# The Encke Gap



October 25, 2004

R. T. Mitchell

12

# SOI Risk Management

## Design

- S/C designed to be largely single fault tolerant
- Operate in flight demonstrated envelope, with margin
- Strict compliance with requirements & flight rules

## Test

- Baseline, fault & stress testing using flight system testbeds (H/W & S/W)
- In-flight checkout & demos to remove first time events

## Failure Analysis

- Critical event driven fault tree analysis
- Risk mitigation & development of contingencies

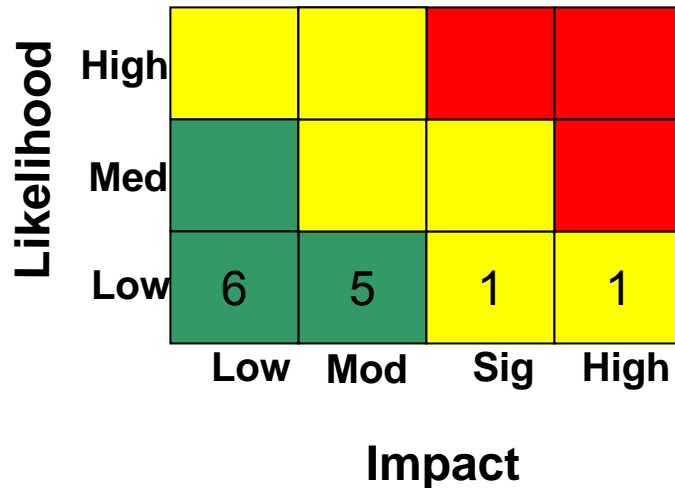
## Residual Risks

- Accepted pre-launch waivers to Single Point Failures
- Unavoidable risks (e.g. natural environment)

## Mission Assurance

- Strict process for characterization of variances (ISAs, PFRs & Waivers)
- Full time Mission Assurance Manager reports to Program Manager
  - Independent assessment of compliance with institutional standards
  - Oversight & risk assessment of ISAs, PFRs & Waivers etc.
  - Risk Management Process facilitator

# SOI Risk Management



## LIKELIHOOD

**High** Risk Event is likely to occur ( $\geq 10\%$  probability)

**Med** Risk Event may occur ( $< 10\%$  probability)

**Low** Risk Event is unlikely to occur ( $< 1\%$  probability)

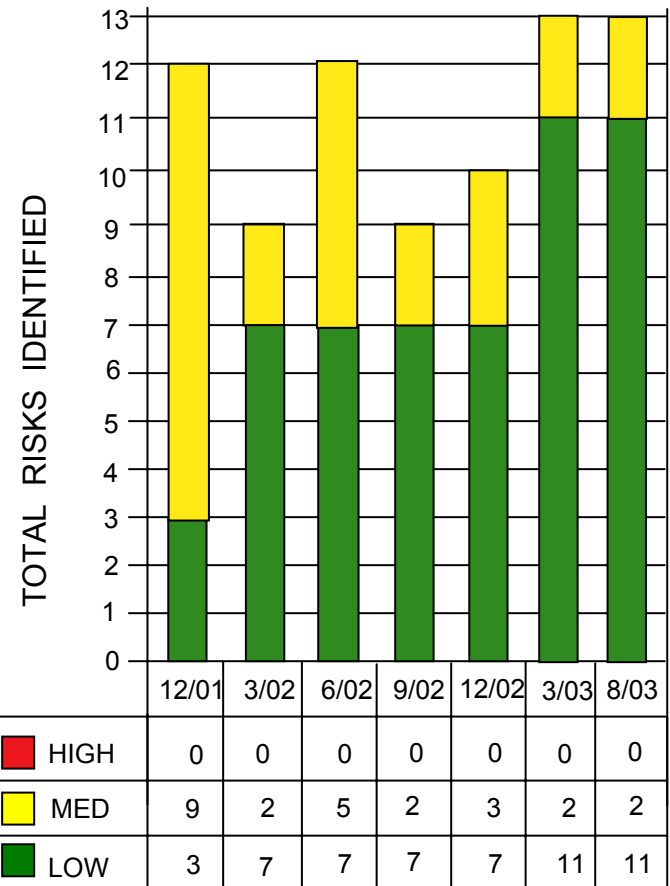
## IMPACT

**High** Impact not repairable within allocated resources

**Sig** Impact may not be repairable within allocated resources

**Mod** Impact may be repairable within allocated resources

**Low** Impact of occurrence easily repairable within allocated resources



# Significant Risk List Assessment

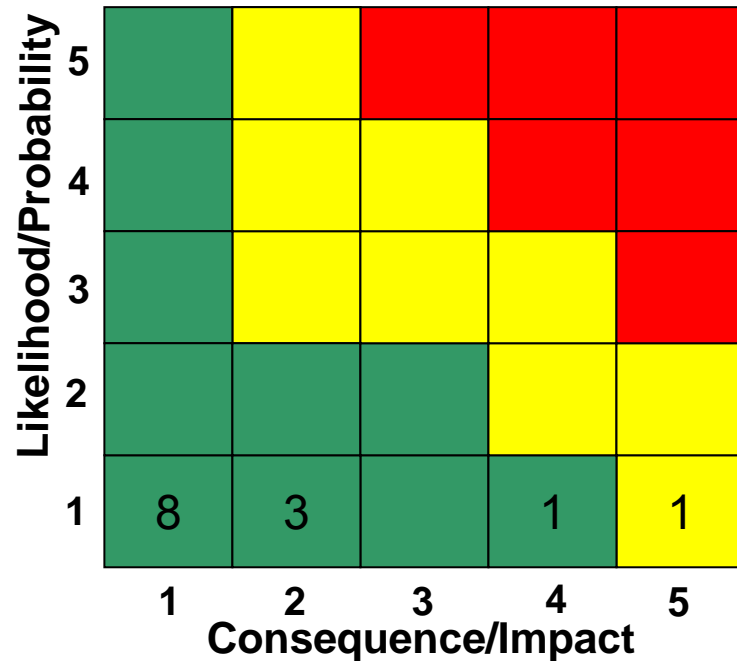
## SOI Risks

ID	Likelihood	Impact	Status	Title
29	1	4	Evaluated	Ring Particle Collision - S/C
35	1	1	Evaluated	S/C Fault Detected Prior to SOI
36	1	1	Evaluated	Loss of D/L Prior to SOI
37	1	1	Evaluated	Loss of Commandability Prior to SOI
39	1	1	Evaluated	Loss of Primary Pressure Reg - SOI
40	1	2	Evaluated	Main Engine Cover Sticks
41	1	2	Evaluated	Failure to Communicate After SOI
43	1	3	Evaluated	Partial SOI Execution
45	1	2	Evaluated	Large SOI Navigation Errors
46	1	2	Evaluated	Loss of Main Engine During SOI
106	1	2	Evaluated	Anomalous PMS Pressurization/TCM-20
107	1	1	Evaluated	Anomalous TCM-21
113	1	1	Evaluated	Sun Sensor Particle Impact

# Significant Risk List Assessment

(Continued)

## SOI - OSMS 5X5 Risk Assessment

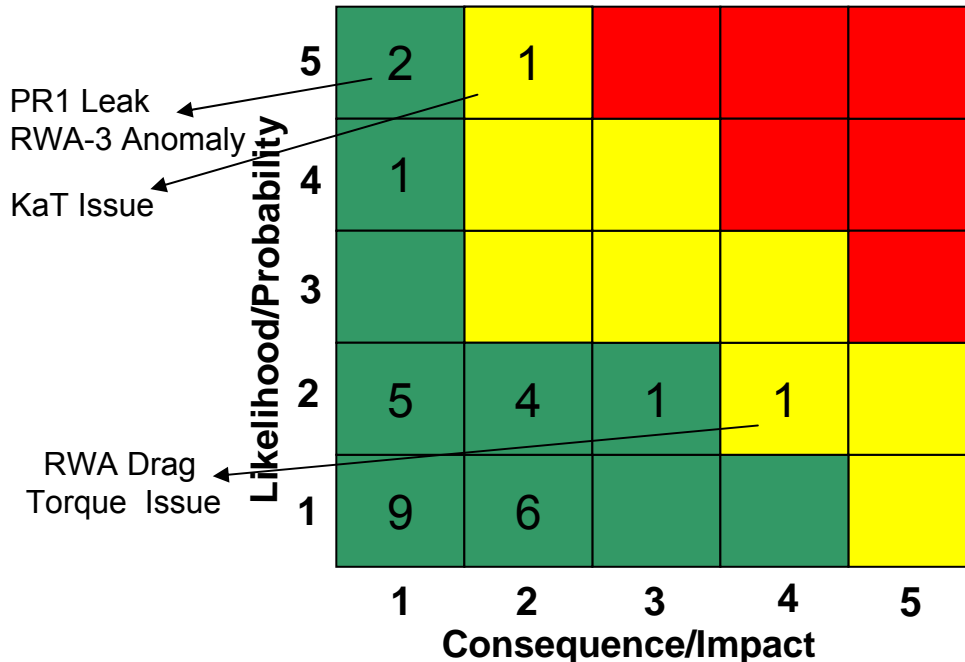


Likelihood
1 Very Low
2 Low
3 Moderate
4 High
5 Very High

Consequence/Impact
1 Minimal or no impact to mission
2 Small reduction in mission return
3 Moderate reduction in mission return
4 Significant reduction in mission return
5 Mission failure

# Red Flag PFR/ISA & Technical Risk Assessment

## Mission - OSMS 5X5 Risk Assessment



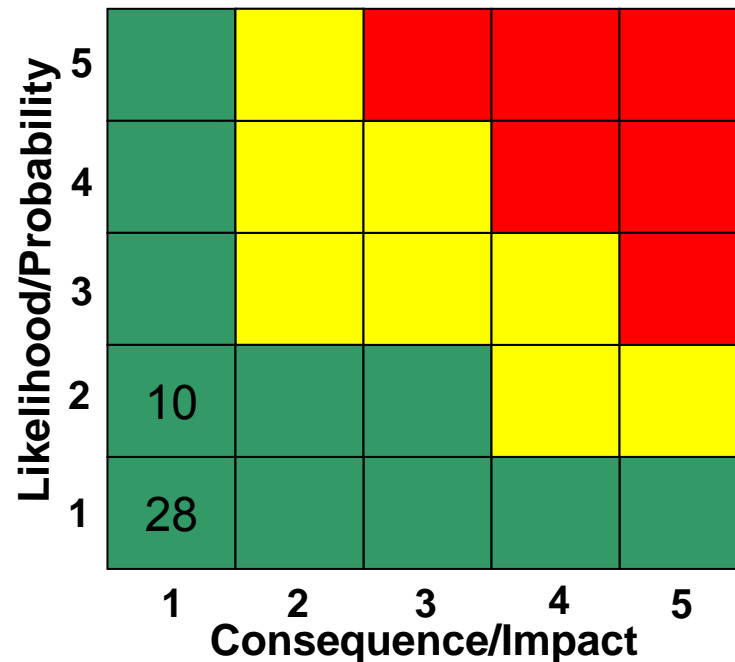
Likelihood
1 Very Low
2 Low
3 Moderate
4 High
5 Very High

Consequence/Impact
1 Minimal or no impact to mission
2 Small reduction in mission return
3 Moderate reduction in mission return
4 Significant reduction in mission return
5 Mission failure

- 31 Red Flag PFRs were written during prelaunch development
  - 7 risk assessed as retired and not included in the matrix
- 1 Red Flag PFR has been documented since Launch
  - Regulator Leakage (PR1), most likely due to particulate contamination
- 5 Technical Risks from OSMS Risk List
  - Probe Receiver RF design flaw - Resolved by redesign of Probe Mission
  - Ka-Band Translator (KaT) anomalous behavior - Reoccurred in 2003 & 2004
  - Narrow Angle Camera Contamination - Corrected by decontamination
  - RWA-3 Drag Torque Issue - Now on RWA 1,2 & 4
  - RWA Drag Torque Issue - RWA-4 has now exhibited some drag torque spikes

# Pre-Launch Waiver Risk Assessment

- Reviewed
  - 18 Potentially SOI related waivers
  - 20 Waivers with dissent / greater than low risk



**No Significant Risk Items Identified for SOI**

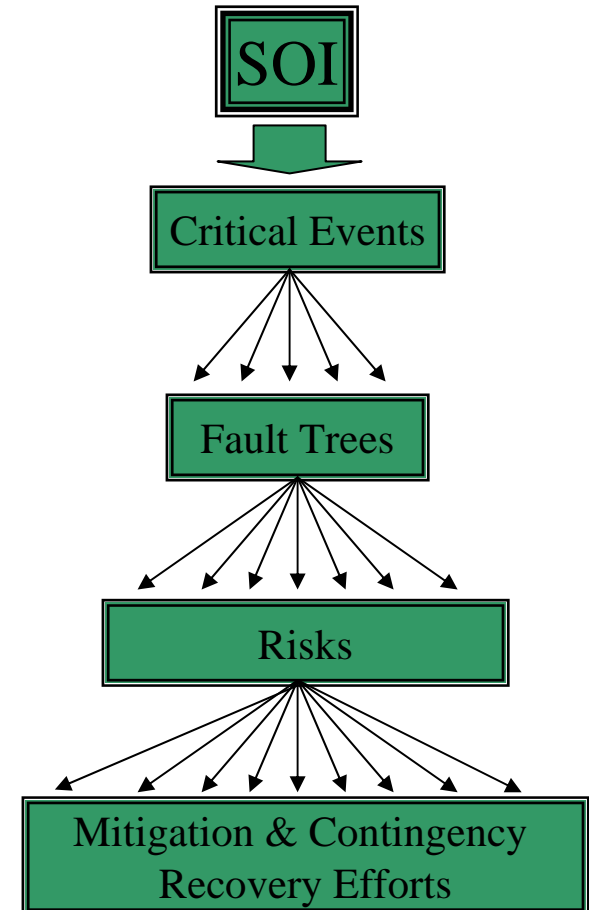
# Risk Identification & Mitigation

## Pre Launch

- Prelaunch Risk Management Process
- FMECAs used extensively
  - S/C designed to be single fault tolerant
  - Limited Single Point Failures (SPF) waived prelaunch

## Post Launch

- Continued Flight S/W development & test
  - Extensive FSW & fault protection upgrades
- SOI Critical Sequence development, analysis & test
  - 2 additional SPFs identified & S/W mods to mitigate
- Top down fault tree / event tree analysis
  - Critical Events & potential faults identified
  - Mitigation efforts and contingencies developed
- Detailed risks and mitigation efforts documented
  - Mission risks in programmatic Sig Risk List (SRL)
  - Off nominal fault tree results captured
  - Additional ground response / contingency plans developed



# Independent Assessment

## Extensive Peer Reviews and Testing

- Peer Reviews preceded every major Design/Risk Review
- SOI Critical Sequence was under strict configuration control
- The sequence was tested and retested extensively
- Additional validation performed in-flight on the S/C
- Critical Events and Fault Scenarios identified & validated
- Addition & validation of AACS “Smartburn” Algorithm
- Flight Software changes for additional Fault Protection

## Independent Reviews

- SOI Preliminary Design Review - October 2000
- “Smartburn” Flight Software Algorithm Review - November 2001
- Critical Sequence Design/Risk Review - February 2002
- SOI Risk Review - October 2003
- SOI Critical Events Readiness Review - April 2004



# In-Flight Validation Activities

## First Time Events

- First time events identified as potential risk areas
- Mitigated risk by demonstrating in-flight

## In Flight Verification

- SOI Critical Sequence Demonstration
  - July 2003
- TCM-19 - May 2003
  - Main Engine (ME) cover closure at 126 seconds
  - Use of both ME engines simultaneously
  - Verified heater usage after end of burn
- TCM-19b - November 2003
  - Validation of “Smartburn” Algorithm, with energy based burn termination
- TCM-20 - May 2004
  - First burn on SOI AACS Flight Software Load (A8.6.7)
  - First long burn with MAG boom deployed



# **JPL & NASA Ops Lessons Learned**

- **JPL Lessons Learned Reviewed for Operations**
  - 36 Ops Lessons Identified and Reviewed
  - No Non-Compliances
- **NASA Lessons Learned Reviewed for Operations**
  - 6 Ops Lessons Identified and Reviewed
  - No Non-Compliances
- **1 Maneuver Contingency Window Added**
  - Additional Maneuver (TCM-22) Scheduled
  - Added upon reviewing LL #916 (MCO)
  - Added capability to add still another maneuver, if needed
- **Verified Lessons are incorporated into Cassini Design**
  - No Residual Risk Areas

# Institutional Compliance Assessment

- **Flight Project Practices**

- 10 Non-Compliances Noted
- All are management practices
- Residual Risk - Low

- **JPL Design Principles**

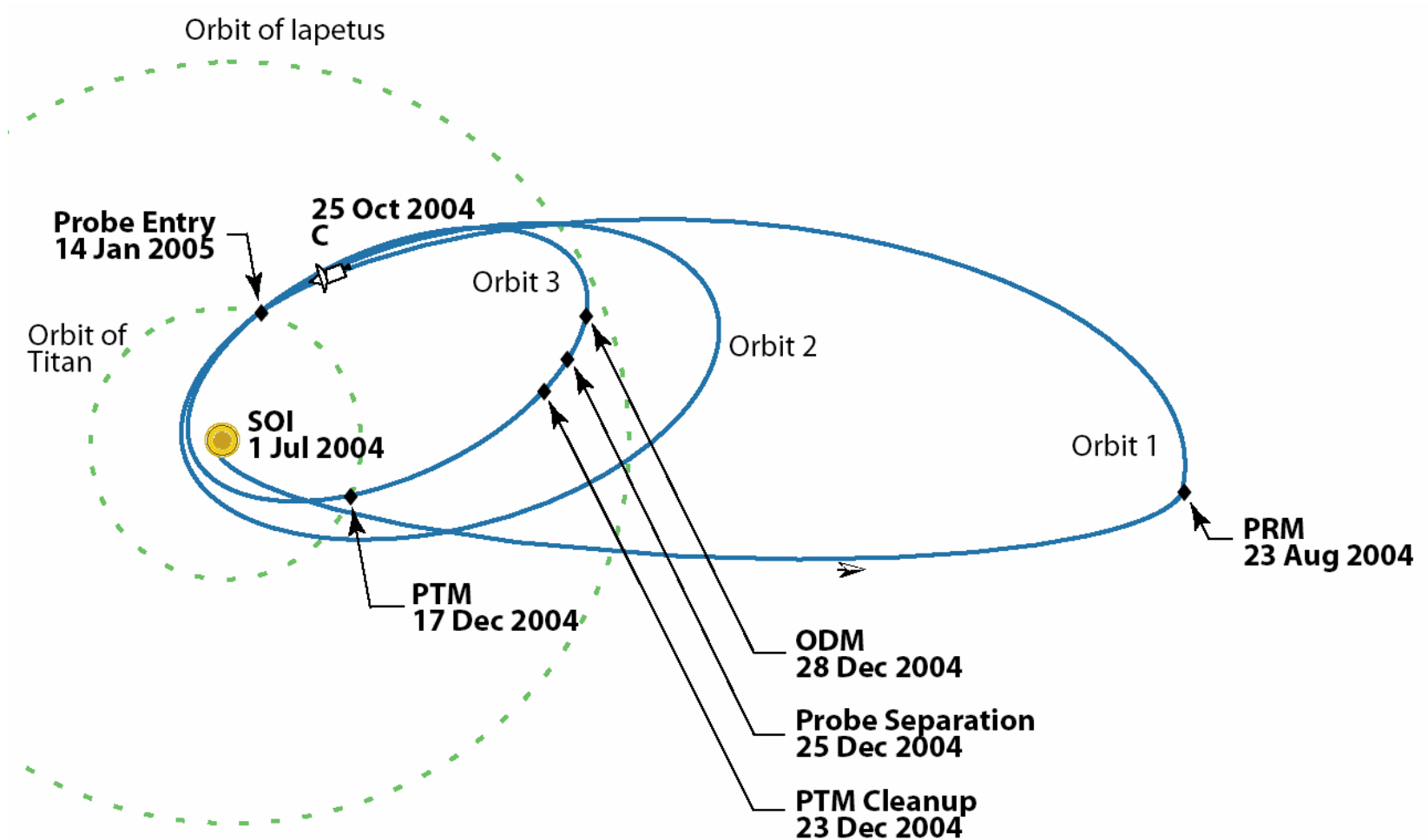
- 5 Non-Compliances Noted
- 5 Cat A Waivers Approved
- Residual Risk - Low

- **JPL & NASA Operations Lessons Learned**

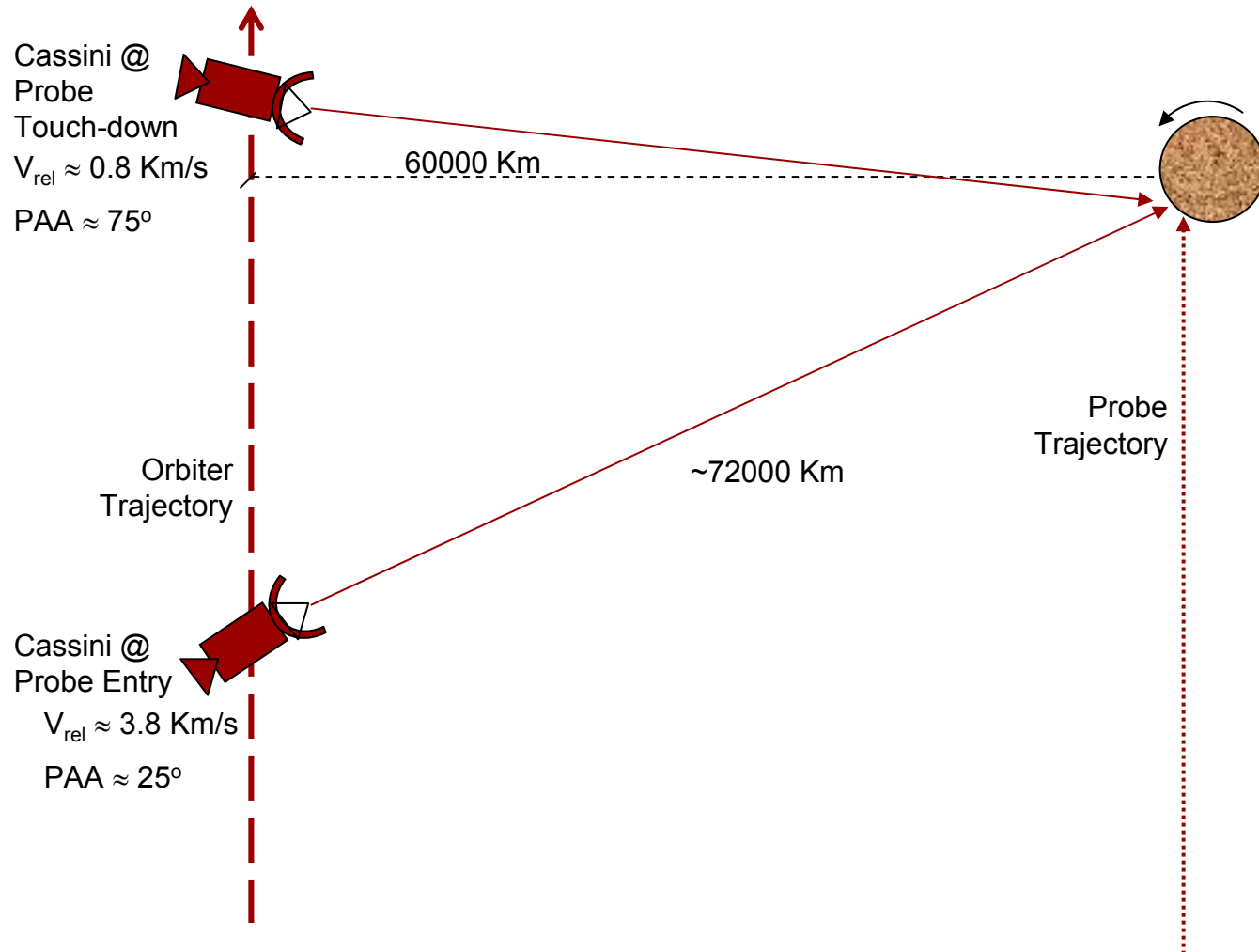
- No Non-Compliances
- Residual Risk - Low

**No Technical Risks for SOI Identified**

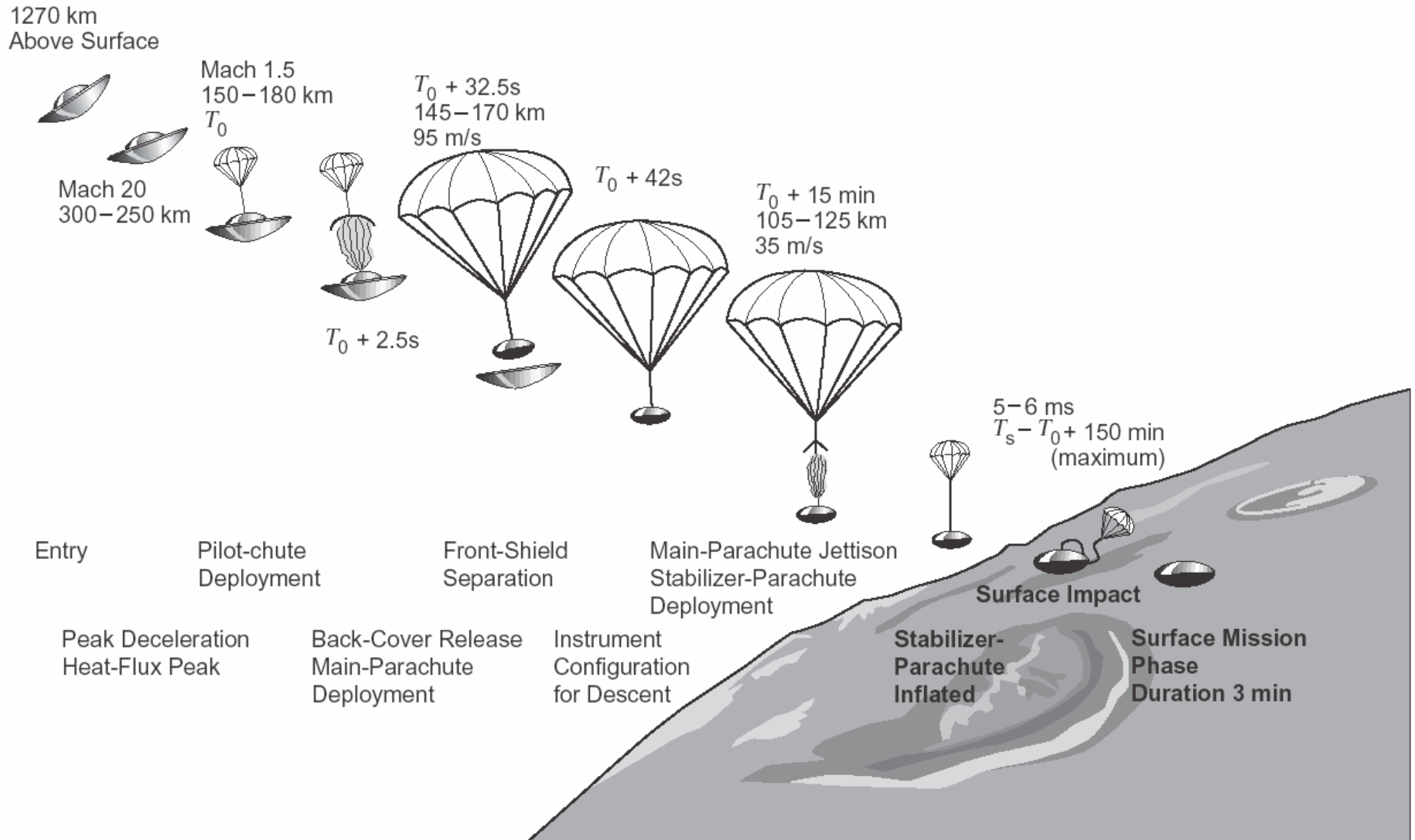
# SOI to Huygens Entry



# Huygens Relay Geometry



# Huygens Descent to Titan



October 25, 2004

R. T. Mitchell

26

# SRL Assessment

## Probe Risks

(Continued)

Likelihood				
	Low	Mod	Sig	High
	High			
	Med	1	1	
Low	Low	3	10	3
	High	3	3	3

### Impact

#### LIKELIHOOD

**High** Risk Event is likely to occur ( $\geq 10\%$  probability)

**Med** Risk Event may occur ( $< 10\%$  probability)

**Low** Risk Event is unlikely to occur ( $< 1\%$  probability)

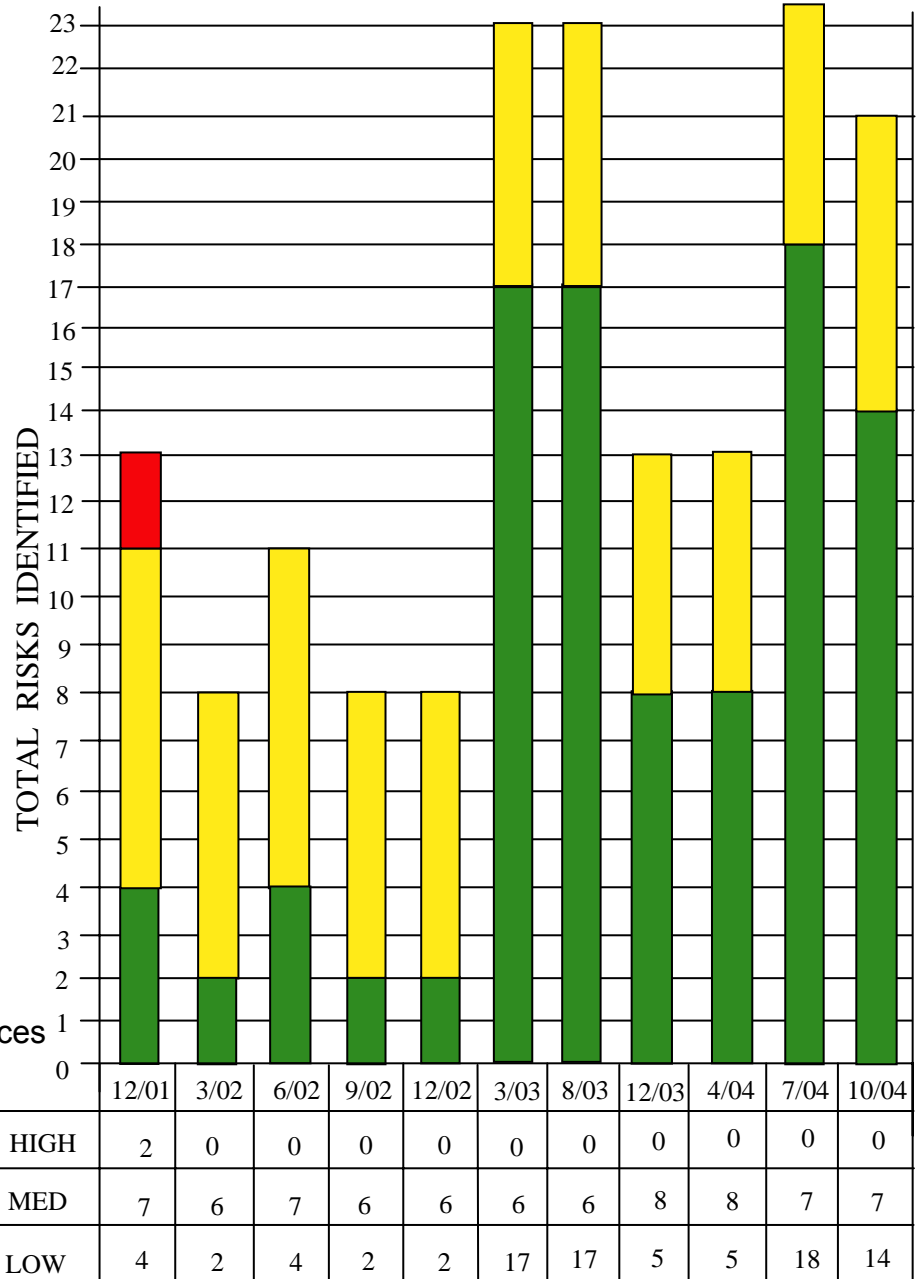
#### IMPACT

**High** Impact not repairable within allocated resources

**Sig** Impact may not be repairable within allocated resources

**Mod** Impact may be repairable within allocated resources

**Low** Impact of occurrence easily repairable within allocated resources



# Probe Risk Identification / Mitigation

Serial Number: 58 Revision: 8

## Risk Item Identification

Contact: mwithkowski

Date Identified: 2001-08-03

Assigned To: sco

Risk Title: Failure to Execute ODM

Description of Risk:

Failure to execute the Orbiter Deflection Maneuver would cause the orbiter to follow the probe into the atmosphere of Titan, and would be mission-catastrophic for both orbiter and probe missions.

Mission Phase: Probe

Other Affected Mission Phases: Not Applicable

## Qualitative Assessment of Impact and Likelihood

Likelihood (without mitigation):

Low - Risk event is unlikely to occur (<1% probability of occurrence).

Impact (without mitigation):

High -

Mission Success

-Impact of occurrence is not repairable within allocated resources

-Major impact to achievement of Mission Objectives

-Major degradation in functionality or performance

-May require major rework or redesign

Schedule

-Schedule slip > 2 months to major milestones

Cost

-Cost overruns > \$500K

## Mitigation Options(s):

Description of All Risk Mitigation Options/Identifying suggested Best Option:

1) Perform extensive ground testing of the ODM sequence to insure that no sequencing errors will abort the maneuver. 2) Design backup and contingency maneuver opportunities into the timeline to insure that opportunities exist to perform the ODM in the event that maneuver fails to execute at the prime opportunity. There are two opportunities to complete the ODM under nominal conditions. Two contingency maneuver windows have been identified and placed in the background sequence. There are multiple opportunities to complete this maneuver if necessary, although some background science activities would be sacrificed.

## Qualitative Residual Assessment of Impact and Likelihood:

Likelihood (with mitigation):

Low - Risk event is unlikely to occur (<1% probability of occurrence).

Impact (with mitigation):

High -

Mission Success

-Impact of occurrence is not repairable within allocated resources

-Major impact to achievement of Mission Objectives

-Major degradation in functionality or performance

-May require major rework or redesign

Schedule

-Schedule slip > 2 months to major milestones

Cost

-Cost overruns > \$500K

Recommended Action: Mitigate

Why the Recommended Action should be chosen:

Implement both mitigation options. Both of these mitigation options have minimal impact on the budget and on the work load of the flight team, and while neither action mitigates against the severity of the impact if this risk is realized, both actions make the likelihood of this mission- catastrophic event occurring even smaller.

## Manager Status/Action(s):

Status of this Risk item: Evaluated

## Risk Exposure Dates:

Milestone Type	Date (YYYY-MM-DD)	Event/Milestone	Milestone Complete
Open	2004-12-24	Probe Release	No
Close	2004-01-14	Probe Relay	No

## Comments:

This risk is addressed under the Failure to Achieve a Tour TCM/ OTM risk statement. M.Witkowski 01/30/02  
Risk returned to Pending Status. M.Witkowski 02/10/03

Last Updated by: mwithkowski (2004-10-20) - Open

# Significant Risk List (SRL) Assessment

## Probe Risks

Risk ID	Likelihood	Impact	Status	Title
47	L	Mod	Evaluated	S/C Fault Prior to Probe Release
48	L	Sig	Evaluated	S/C Fault Prior to Probe Relay
53	M	Mod	Evaluated	Slow Orbit Determination Convergence
54	L	Sig	Evaluated	Anomalous Probe Release
55	L	Mod	Evaluated	Failure to Separate Probe
56	L	Sig	Evaluated	Miss Probe Release at Tc Opportunity
57	L	Mod	Evaluated	Anomalous Orbit Deflection Maneuver
58	L	High	Evaluated	Failure to Execute ODM
59	L	High	Evaluated	Loss of Link During Probe Relay
97	L	Mod	Evaluated	Anomalous Final Probe Checkout
98	L	Low	Evaluated	Anomalous Mission Timer Unit test
99	L	Mod	Evaluated	Anomalous Battery Depassivation
101	L	Mod	Evaluated	Anomalous Tb Approach Maneuver
102	L	Mod	Evaluated	Anomalous PTM
103	L	Mod	Evaluated	Anomalous MTU Loading
104	L	Low	Evaluated	Iapetus C Orbiter Science
105	L	Low	Evaluated	Late Probe Pointing Udate
130	L	Mod	Evaluated	Probe Mission Dependence-BKG SEQ
131	Med	Low	Evaluated	Loss of DSN Track
132	Low	Mod	Evaluated	Titan Atmosphere Model Update
133	L	High	Evaluated	AACS FSW Autonomous Unmute